Information on the Unauthorized Disclosure of Classified or Controlled Unclassified Information ("CUI")

In an effort to limit unauthorized disclosures of classified or Controlled Unclassified Information (CUI), the White House has tasked all federal agencies with reinforcing key concepts in the handling and protection of classified information and CUI. It is important to keep in mind that unauthorized disclosures can have serious consequences to national security. Enemies of the United States are relentless in their pursuit of information which they can exploit to harm US interests. Therefore, federal employees, federal contractors and specifically assigned personnel, have a special responsibility to properly protect classified information and CUI from any unauthorized disclosure.

None of the prohibitions cited below are meant to discourage legitimate disclosures, through the proper channels, of fraud, waste and abuse, as well as violations of law, rules and regulations. EPA personnel who disclose these issues are protected by federal law, including the Whistleblower Protection Enhancement Act of 2012, and are encouraged to report the discrepancies through the EPA OIG Hotline at 888-546-8740.

I. Types of unauthorized disclosure include:

Espionage - using spies to obtain information about the plans and activities especially of a foreign government or a competing company. Example: In the mid-1980's Aldrich Ames, a counter-intelligence officer at the CIA, disclosed classified information to the KGB on Russian nationals clandestinely working for the US. At least 10 operatives were executed as a result of the information provided, seriously impacting US intelligence operations in the Soviet Union.

Hacks – intentionally accessing a computer system or network without authorization or exceeding the level of authorized access. Example: in June 2015, OPM announced that it had been the target of a data breach which impacted up to 18 million people. Compromised information included names, Social Security numbers, dates/places of birth, home addresses, and detailed security-clearance-related background information. Possessing such information can assist an adversary in targeting or exploiting individuals whose personal data was stolen.

Leaks – the unauthorized disclosure of classified information or CUI to the media. Example: in 1972, Washington Post columnist Jack Anderson disclosed that US intelligence was intercepting sensitive telephone conversations between limousines used by members of the Soviet Politburo. The highly successful program abruptly ended shortly after the disclosure.

II. Protecting CUI and Classified Information

A. CUI:

Federal agencies routinely generate, use, store, and share information that, while not meeting the standards for classified national security information, requires safeguarding and dissemination controls pursuant to a law, regulation, or government-wide policy. This type of information, which includes Personally Identifiable Information (PII), is now under the term of Controlled Unclassified Information (CUI).

CUI is unclassified information that meets the standards for safeguarding and dissemination controls per law, regulations, and government-wide policies under 32 CFR 2002. Previously,

similar information may have been referred to as Sensitive but Unclassified (SBU) or For Official Use Only (FOUO).

An example (other than PII) of CUI that the EPA receives is information that Industry claims as Confidential Business Information (CBI). This information may be CUI and need protection.

While specific implementing guidance at the EPA is under development, steps required to protect CUI include:

- understanding and identifying CUI;
- only disseminating CUI to authorized holders (i.e. individuals who are permitted access under the law, regulation, or government-wide policy; have a lawful government purpose in accessing the information; and for whom an authorized limited dissemination control does not restrict access);
- ensuring that if CUI is to be released outside the Agency, then it is marked appropriately;
- securing CUI by appropriate means, which may differ by type;
- following the incident reporting process if CUI is found unprotected.

If you have any questions regarding the protection of CUI, please contact Lauren Gordon, CUI Program Manager at 202-566-0613.

B. Classified Information:

Protecting classified information is a serious responsibility. Each EPA employee who has authorized access to classified information must sign an SF 312 Non-Disclosure Agreement Form, a legally binding agreement between the cleared employee and the government. The SF 312 is a written acknowledgement that the employee understands the trust that the government has placed in them by granting them access to classified information. It also indicates the employee accepts the described responsibilities to protect national security information and states that there are criminal and civil consequences for not complying with the rules pertaining to unauthorized disclosure. Those penalties range from withdrawal of the security clearance to imprisonment.

Additional federal and agency requirements also prohibit unauthorized disclosure of classified information. Specifically, 32 C.F.R. 2001.40 states, "(a) Classified information, regardless of its form, shall be afforded a level of protection against loss or unauthorized disclosure commensurate with its level of classification." Agency guidance is found in the NSI Handbook, Version 2, 2012 Chapter 5, 5-300 "General Restrictions on Access", which states that a person may have access to classified information provided that "a favorable determination of eligibility for access to classified information has been made, they have been in-briefed and have signed a Classified Information Non-Disclosure Agreement Form (SF-312), and they have a valid need-to-know."

It is important to remember that no cleared individual has a right to gain access to classified information solely by virtue of title, position, or level of security clearance. If you hold classified information, you should not assume that simply because an individual requests access to that information, they have the appropriate clearance and need-to-know. Clearances must be verified by contacting the Personnel Security Branch at 202-564-7912. If you are unsure of an individual's need-to-know, speak with your supervisor or lead for the project you are working on.

If you wish to discuss classified information, or review classified documents at the EPA, you can only do so in an area accredited for classified discussion and/or review. In addition, classified information may only be electronically transmitted using an authorized information system approved for the level of material you wish to share; Homeland Secure Data Network (HSDN) for information up to the Secret level; the Joint Worldwide Intelligence Communication System (JWICS) for information up to the Top Secret/SCI level. If you are unsure where to find a room accredited for a specific classified operation, contact your NSI Representative or the NSI Program Team.

You should also consider the risk of inadvertent disclosure. If you are having a classified discussion, anyone else who may be in the secure room should be asked to leave unless they have a valid-need-to-know. Further, never attempt to "talk around" classified information as you may inadvertently divulge material which requires protection.

Unauthorized Disclosure
Discussion Topics for Managers

Introduction

We are here today to talk about the importance of protecting from unauthorized disclosure, classified or other sensitive US government information, known as Controlled Unclassified Information or "CUI". As federal employees, federal contractors or specifically assigned personnel, we all handle government information as a function of our work at EPA. As stewards of this information, we should always remember that:

- Unauthorized disclosures can have serious consequences to national security.
- Enemies of the United States are relentless in their pursuit of information which they can exploit to harm US interests.
- As members of the federal workforce, we have a special responsibility to properly protect classified information and CUI from any unauthorized disclosure.

Whistleblowing

Keep in mind that the prohibitions we will discuss do not refer to "Whistleblowing". Whistleblowing is defined as the lawful disclosure of information that an employee reasonably believes evidences: a violation of any law, rule or regulation; gross mismanagement; gross waste of funds; an abuse of authority; a substantial and specific danger to public health or safety; or censorship related to scientific research or analysis. Agency employees have the right to make lawful disclosures to anyone, including, for example, management officials, the Inspector General, and/or the Office of Special Counsel. Employees may make disclosures to the EPA Office of the Inspector General through the EPA OIG Hotline at 888-546-8740.

What is "Unauthorized Disclosure"?

Providing or making information available to individuals or entities, whether intentional or otherwise, which they are not authorized to view or possess, pursuant to law, executive order, regulation, Government-wide policy, or directives.

Examples of unauthorized disclosure include:

Espionage - using spies to obtain information about the plans and activities especially of a foreign government or a competing company.

Example: in the mid-1980's, Aldrich Ames, a CIA counter-intelligence officer, disclosed classified information to the KGB on Russian nationals clandestinely working for the US. At least 10 operatives were executed as a result of the information provided, seriously impacting US intelligence operations in the Soviet Union.

Hacks – intentionally accessing a computer system or network without authorization or exceeding the level of authorized access.

Example: in June 2015, OPM announced that it had been the target of a data breach which impacted up to 18 million people. Compromised information included names, Social Security numbers, dates/places of birth, home addresses, and detailed security-clearance-related

background information. Possessing such information can assist an adversary in targeting or exploiting individuals whose personal data was stolen.

Leaks – the unauthorized disclosure of classified information or CUI to the media.

Example: in 1972, Washington Post columnist Jack Anderson disclosed that US intelligence was intercepting sensitive telephone conversations between limousines used by members of the Soviet Politburo. The highly successful program abruptly ended shortly after the disclosure.

Watch video:

http://video.foxnews.com/v/5534515368001/?#sp=show-clips

Description: An interview with the Director of the National Counterintelligence and Security Center, William Evanina regarding unauthorized disclosures. He discusses the difference between leaks and whistleblowing, and damage to national security caused by the unauthorized leaking of classified or sensitive government information.

Preventing Unauthorized Disclosures

Protecting CUI:

CUI is:

- Unclassified information that meets the standards for safeguarding and dissemination controls per law, regulations, and government-wide policies under 32 CFR 2002.
- Information that, while not meeting the standards of classified national security information, still requires safeguarding and dissemination controls.
- Information that may previously have been referred to as Sensitive but Unclassified (SBU) or For Official Use Only (FOUO). (Note, however, that CUI may include more information than that which was SBU and FOUO; and not all SBU and FOUO will be categorized as CUI).

All CUI is subject to the safeguarding and dissemination controls established in the Federal CUI Registry. Unauthorized disclosure, depending on the underlying law or regulation, may result in penalties to the individual making such disclosure and to the agency as a whole. EPA is currently developing specific guidance for the protection and dissemination of CUI.

Examples of CUI, include:

- Personally Identifiable Information
- Confidential Business Information
- Controlled Technical Information
- Critical Infrastructure Information
- Information System Vulnerability Information

- Law Enforcement Information

A complete list of CUI categories of can be found at:
https://www.archives.gov/cui/registry/category-list.html

How to protect CUI:

- Understand what CUI is;
- Review the National Archives and Records Administration Information Security Oversight Office CUI Registry - https://www.archives.gov/cui/registry/category-list to determine if the CUI needs only the basic level protection or if it requires specified protection (e.g., PII protection is specified; some Industry designated CBI is also specified)
- Only disseminate CUI to authorized holders (i.e. individuals who are permitted access under the law, regulation, or government-wide policy; have a lawful government purpose in accessing the information; and for whom an authorized limited dissemination control does not restrict access);
- Ensure that if CUI is to be released outside the Agency, that it is marked appropriately;
- Don't leave it in the open (lock it up or retain actual physical possession);
- Follow security's incident reporting process if it is found unprotected.

If you have any questions regarding the protection of CUI, please contact Lauren Gordon, CUI Program Manager on 202-566-0613.

Watch video:

https://www.c-span.org/video/?432127-1/attorney-general-says-culture-leaking-muststop&live

Description: Attorney General Jeff Sessions announced new plans to crack down on those who leak classified information. The attorney general says that the leaking of classified information has “exploded.” He warned that the “culture of leaking must stop.”

Protecting Classified Information

SF 312 Non-Disclosure Agreement Form:

Those of you with a security clearance were required to sign a SF 312 Non-Disclosure Agreement Form. The SF 312:

- Is a legally binding agreement between the cleared employee and the government.
- Is a written acknowledgement that the employee understands the trust that the government has placed in them by granting them access to classified information.
- Indicates the employee accepts the described responsibilities to protect national security information.

Unauthorized Disclosure
Discussion Topics for Managers

- States that there are criminal and civil consequences for not complying with the rules pertaining to unauthorized disclosure; those penalties range from withdrawal of the security clearance to imprisonment.

Access to classified information:

- Requires a current security clearance and an official need-to-know.
- No individual has a right to gain access to classified information solely by virtue of title, position, or level of security clearance.
- Clearances must be verified by contacting the Personnel Security Branch at 202-564-7912.
- If you are unsure of an individual's need-to-know, speak with your supervisor or lead for the project you are working on.

Conducting Classified Operations:

- Can only be performed in a space properly accredited for the classified operation in question (such as discussion or review); different accredited spaces are approved for different types of classified operations.
- Classified information may only be electronically transmitted using an authorized information system (Homeland Secure Data Network or Joint Worldwide Intelligence Communication System) located in an accredited space, and approved for the level of material you wish to share.
- If you are unsure where to find a room accredited for a specific classified operation, contact your NSI Representative or the NSI Program Team.

Preventing Inadvertent Disclosure:

- If you are having a classified discussion, anyone else who may be in the secure room should be asked to leave unless they have a valid-need-to-know.
- Never attempt to "talk around" classified information as you may inadvertently divulge material which requires protection.

Take Training:

https://securityawareness.usalearning.gov/unauthorizedrefresher/index.htm

This course provides an overview of what unauthorized disclosure is, including specific types of unauthorized disclosure and some common misconceptions about unauthorized disclosure. This course will also discuss the types of damage caused by unauthorized disclosure and the various sanctions one could face if caught engaging in unauthorized disclosure.

In closing, unauthorized disclosure of classified or Controlled Unclassified Information (CUI) causes harm to the United States and impacts the confidence of the American people in our government. As federal employees, federal contractors, and specially assigned personnel, we are

required to protect information that has not been authorized for dissemination outside of the federal government. Doing so protects not only the EPA, but the security of the nation as a whole.